

<b>PRE-APPEAL BRIEF REQUEST FOR REVIEW</b>		Docket Number (Optional) 44655-306460			
<p>I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)]</p> <p>on _____</p> <p>Signature _____</p> <p>Typed or printed name _____</p>		Application Number 10/689,549	Filed 21 Oct 2003		
		First Named Inventor Joona AIRAMO			
		Art Unit 2132	Examiner HOMAYOUNMEHR, Farid		
<p>Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.</p> <p>This request is being filed with a notice of appeal.</p> <p>The review is requested for the reason(s) stated on the attached sheet(s). Note: No more than five (5) pages may be provided.</p> <p>I am the</p> <table style="width: 100%; border: none;"><tr><td style="width: 50%; vertical-align: top; padding: 5px;"><p><input type="checkbox"/> applicant/inventor.</p><p><input type="checkbox"/> assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)</p><p><input checked="" type="checkbox"/> attorney or agent of record.      41,844 Registration number _____</p><p><input type="checkbox"/> attorney or agent acting under 37 CFR 1.34. Registration number if acting under 37 CFR 1.34 _____</p></td><td style="width: 50%; vertical-align: top; padding: 5px;"><p>/ Christine H. McCarthy /</p><p style="text-align: center;">_____ Signature</p><p>Christine H. McCarthy</p><p style="text-align: center;">_____ Typed or printed name</p><p>(202) 289-1313</p><p style="text-align: center;">_____ Telephone number</p><p>February 21, 2008</p><p style="text-align: center;">_____ Date</p></td></tr></table> <p>NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.</p>				<p><input type="checkbox"/> applicant/inventor.</p> <p><input type="checkbox"/> assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)</p> <p><input checked="" type="checkbox"/> attorney or agent of record.      41,844 Registration number _____</p> <p><input type="checkbox"/> attorney or agent acting under 37 CFR 1.34. Registration number if acting under 37 CFR 1.34 _____</p>	<p>/ Christine H. McCarthy /</p> <p style="text-align: center;">_____ Signature</p> <p>Christine H. McCarthy</p> <p style="text-align: center;">_____ Typed or printed name</p> <p>(202) 289-1313</p> <p style="text-align: center;">_____ Telephone number</p> <p>February 21, 2008</p> <p style="text-align: center;">_____ Date</p>
<p><input type="checkbox"/> applicant/inventor.</p> <p><input type="checkbox"/> assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)</p> <p><input checked="" type="checkbox"/> attorney or agent of record.      41,844 Registration number _____</p> <p><input type="checkbox"/> attorney or agent acting under 37 CFR 1.34. Registration number if acting under 37 CFR 1.34 _____</p>	<p>/ Christine H. McCarthy /</p> <p style="text-align: center;">_____ Signature</p> <p>Christine H. McCarthy</p> <p style="text-align: center;">_____ Typed or printed name</p> <p>(202) 289-1313</p> <p style="text-align: center;">_____ Telephone number</p> <p>February 21, 2008</p> <p style="text-align: center;">_____ Date</p>				
<p><input type="checkbox"/> *Total of _____ forms are submitted.</p>					

This collection of information is required by 35 U.S.C. 132. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11, 1.14 and 41.6. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of  
JOONA AIRAMO

Group Art Unit: 2132

Appln. No.: 10/689,549

Examiner: HOMAYOUNMEHR

Filed: October 21, 2003

Title: DETECTING AND BLOCKING MALICIOUS CONNECTIONS

\* \* \* \* \*

ATTACHMENT SHEETS FOR PRE-APPEAL BRIEF REQUEST FOR REVIEW

**MAIL STOP AF**

Commissioner for Patents  
P.O. Box 1450  
Alexandria, Virginia 22313-1450

Sir:

Appellant hereby requests that a panel of examiners formally review the legal and factual basis of the rejections in the above-identified application prior to the filing of an appeal brief.

**STATUS OF CLAIMS**

By the October 4, 2007, Final Rejection, claims 1, 6, 8, 13 and 14 remain rejected under 35 U.S.C. 102(b) as being anticipated by Jain et al. (U.S. 2003/0131116; hereafter "Jain") and claims 2-5, 7, 9-12 and 15 remain rejected under 35 U.S.C. 103(a) as being unpatentable over Jain and Hall (U.S. 2004/0054928). Appellant asserts that these rejections must be overturned because they are based both on errors of law and fact. More specifically, Appellant submits that the Examiner's interpretation of both the claimed invention and the teachings of the cited prior art are factually incorrect and the Examiner's understanding of the requirements of legal anticipation and obviousness is incorrect. Thus, based on a correct factual and legal analysis, the cited prior art fails to teach or suggest all the features recited in the rejected claims. Accordingly, Appellant requests review and withdrawal of the rejections.

## TRAVERSAL OF PRIOR ART REJECTIONS

### NOVELTY OVER JAIN

Appellant has previously asserted that the prior art references, analyzed individually or in combination, fail to teach or suggest the claimed method (independent claim 1), computer readable storage medium (independent claims 8 and 13), device (independent claims 6 and 14), wherein malicious related connections are detected and blocked by examining relationships between a port negotiated for a related connection and the associated control connection, and by deciding on the basis of this relationship, whether the related connections shall be allowed. Appellant further argued that the cited prior art fails to teach or suggest the claimed invention embodiments wherein a port of a device is opened within a predefined time window in relation to noticing negotiation of a related connection within the control connection (as recited in dependent claims 2 and 9) or the claimed invention embodiments wherein a control connection and the port of a device are both opened using the same process family (as recited in dependent claims 3 and 10).

In response to those previously submitted arguments for traversal of the prior art rejections, the Examiner has now boldly discounted the arguments by merely asserting that paragraphs 31-38 of Jain teach the claimed step of checking if the relationship between said port and the device and the control connection fulfills predefined criteria. Specifically, the Examiner asserts that these paragraphs 31 to 38 disclose that a main (control) channel and additional channels and ports are identified by a firewall, and policy is enforced. Thus, under the Examiner's rationale, the "policy" is what constitutes the predetermined criteria against which the device port/control connection relationship is checked.

This analysis and characterization is incorrect.

In fact, paragraphs 31-38 of Jain merely disclose that PDUs of different protocols (e.g. TCP, UDP, FTP) are tagged with different values. Thus, when a specific type of PDU is received at the firewall, it is tagged with a corresponding tag value.

Additionally, within a specific protocol, sub-classification may be performed. For example, the FTP-Get and FTP-Put commands may be sub-classified by dedicated tagged values (see paragraph 33 to 34). For some of the operations in FTP protocol (such as Get) may require an additional channel to be set up. For example, according to paragraph 33, the additional channel is a dynamically negotiated port 114 and "for the purposes of the firewall, this port should be dynamically opened". In other words, Jain merely teaches opening

associated channels unconditionally. Paragraphs 37 and 38 teach that the associated channels may be classified and tagged in a similar manner as the parent channel.

**However, this classifying and tagging has nothing to do with checking the relationship between a port of the device and the control connection against predefined criteria.** This is because **the associated channel or port** is not checked against any predefined criteria. Rather, according to Jain, the associated channel is unconditionally opened when negotiated. Thus, contrary to the Examiner's assertion, there is no mention of any policy that is enforced in paragraphs 31-38.

Appellants recognize that paragraph 45 (not referred to by the Examiner) mentions that common policies are applied to the PDU traffic on a dynamically negotiated and opened F\*TP data channel. However, such policies are applied to traffic on an “already opened channel,” as part of not to the relationship between a port of the device and the control connection against predefined criteria so as to determine whether the connection should be opened at all.

Thus, Jain fails to teach or suggest checking whether relationship between said (negotiated) device port and the control connection fulfills predefined criteria. Accordingly, Jain fails to teach or suggest the claimed invention wherein malicious related connections are detected and blocked by examining relationships between a port negotiated for a related connection and the associated control connection, and by deciding on the basis of this relationship, whether the related connections shall be allowed.

In response to Appellant’s previous asserted argument that Jain fails to teach the step of conditionally blocking the related connection, if the device port does not fulfill the predefined criteria, the Examiner has now asserted that Jain’s paragraphs 138-139 teach this feature because “one of the enforced policies is blocking the connection.”

However, this rationale is factually incorrect. As explained above, Jain fails to disclose, teach or suggest the claimed checking was disclosed, and, in fact, no policy was mentioned in paragraphs 31 to 38. Further, the Examiner’s factual analysis is further flawed because paragraphs 138 and 139 actually teach that individual PDUs are examined and (1) modified, (2) not modified, (3) ignored, or (4) used to actively terminate the connection.

Thus, Jain (in particular at paragraphs 138 and 139) fails to teach or suggest (1) checking whether a relationship between the (negotiated) port of the device and the control connection fulfills predefined criteria, and (2) conditionally blocking the related connection,

if the port of the device does not fulfill the predefined criteria, as recited in independent claim 1, 6, 8 13, and 14 and their respective dependent claims.

NON-OBVIOUSNESS OVER JAIN AND HALL

The Examiner asserted that Hall remedies various deficiencies of Jain by teaching that a port of a device is opened within a predefined time window in relation to noticing negotiation of a related connection within the control connection (pertaining to rejected dependent claims 2 and 9).

However, Hall fails to remedy Jain's deficiency of failing to teach (1) checking whether a relationship between the (negotiated) port of the device and the control connection fulfills predefined criteria, and (2) conditionally blocking the related connection, if the port of the device does not fulfill the predefined criteria, as recited in independent claim 1, 6, 8 13, and 14 and their respective dependent claims.

Therefore, the anticipation and obviousness rejections of the pending claims must be overturned based on the Examiner's misinterpretation of prior art references and its misapplication to claims 1-15.

Please charge any fees associated with the submission of this paper to Deposit Account Number 021010 (44655-306460). The Commissioner for Patents is also authorized to credit any over payments to the above-referenced Deposit Account.

Respectfully submitted,

Barnes & Thornburg LLP

By: / Christine H. McCarthy /

Christine H. McCarthy

Reg. No. 41,844

Tel. No.: (202) 371-6371

Fax No.: (202) 289-1330

February 21, 2008

Barnes & Thornburg LLP  
Suite 900  
750 17<sup>th</sup> Street, N.W.  
Washington, D.C. 20006  
Tel. No.: (202) 289-1313